

APPLICATION
FOR
UNITED STATES LETTERS PATENT

0000000000
TITLE: NETWORK SESSION MANAGEMENT
APPLICANT: ULHAS S. WARRIER AND PRAKASH IYER

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EE647185808US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

March 31, 2000
Date of Deposit

Signature

Peter F. Consoli

Peter F. Consoli
Typed or Printed Name of Person Signing Certificate

NETWORK SESSION MANAGEMENT

This invention relates to network session management.

BACKGROUND

5 A virtual private network (VPN) is a data service that offers transmission characteristics similar to those of private lines using the public Internet. Remote access VPNs can be used for accessing corporate local area networks (LANs) over public networks from small office home offices (SOHO) where employees of the corporations can work from home. The rise of security technologies such as IPSEC, a secure form of the Internet Protocol with optional authentication and encryption, as well as improved quality of service (QoS) has made VPN applications practical. At the same time, the rise in high-speed communication lines such as asymmetric digital subscriber lines (ADSL) and cable modems has increased the vulnerability of the VPNs because they provide conduits for hackers on the public Internet to access sensitive information on a corporate network during a VPN session.

20 IT administrators can impose restrictions on network access privileges of the remote system to the corporate LAN during a VPN session. For example, during a VPN session between a SOHO and a corporate LAN, the home gateway between the SOHO and the LAN might allow the client access to the printer at home but not to the public Internet. In many situations the home office user may wish to re-configure the network resources based on policies delivered from the LAN. 25 VPN clients are not typically home-networking aware and consequently may limit home network usage during VPN sessions. Personal computer (PC) firewalls are configurable, but are not well integrated with VPN clients and cannot enforce dynamic 30 network stack reconfiguration based on policies.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a transaction system.
Fig. 2 illustrates a transaction system with a small home office local area network.
5 Fig. 3 illustrates an embodiment of a network stack.
Fig. 4 is a flow chart of a method of dynamically reconfiguring a network stack during a VPN session.

DETAILED DESCRIPTION

10 As shown in Fig. 1, a transaction system 100 allows for transactions between a home office and a corporation. A client station such as a SOHO 105 can use a browser 110 or other network software to initiate a network transaction. The SOHO 105 uses its network software to connect to the Internet 115. The SOHO 105 can connect to Public Web Servers on Internet/Other network 120 or can initiate a VPN session with a corporate LAN 135 through this connection with the Internet 115 and through the corporate Access server 125. The corporate LAN 135 can be, for example, a local network or expanded network of computers in a single location or a national or even international location. When the SOHO 105 initiates the VPN session, it is connected with other computers associated with the corporate LAN 135 (based on policies set for corporate LAN 135. Various devices 140, 145 are connected to the corporate LAN 135 for access from other devices on the LAN or a SOHO/remote device 105.

25

30 The corporate Access server 125 can include a policy engine 126 having a list of policies that grant privileges to a variety of users. The policy engine 126 is used to create filters 127 that permit or deny users access to the devices 140, 145 on the corporate LAN 135.

Fig. 2 illustrates the system 100 of Fig. 1 with an expanded view of the SOHO 105 as a network 200. A SOHO LAN 205 can have several attached devices including a PC 210 that initiates a VPN session, a printer 215 and other devices 220.

5 During a VPN session, the device that initiated the VPN session also can function as a node in the SOHO network 200. For example, in a typical SOHO network 200, the VPN device 210 can perform the role of a gateway. Other devices such as the PC 225 can access services available on the VPN PC 210, or the VPN PC 210 can access printer 215 or other devices 220 on the SOHO network 200.

10 Sharing the SOHO network 200, however, should not compromise the security of the corporate LAN 135. Other PCs such as the PC 225 should be able to access the corporate LAN 135 through the VPN PC 210. Conversely, other devices 140, 145 on the corporate LAN 135 should not be able to access PCs on the SOHO network 200. If the VPN PC 210 is also the gateway, then other PCs on the SOHO network such as PC 225 should be able to access Public servers or other network 120 without compromising security of the SOHO network 200 or the corporate LAN 135 or any device associated with the VPN session. However, any nodes on the Internet 120, that is, any unauthorized users, should not be able to access any of the services on the VPN PC 210 during the VPN session. Any such access would be a breach of security of the VPN session and must be avoided.

20 To enhance the security of the system, the VPN PC 210 has a network stack component 210b. The network stack component 210b includes data storage locations typically accessed in a sequential manner, and defines the parameters of the VPN session. To provide the security and access parameters discussed above, the network stack is dynamically reconfigured during the VPN session. Reconfiguration can be statically 30 pre-determined or can be dynamically controlled by policies downloaded by the VPN PC 210 from 126 during the VPN session setup. Policies can be fine-grained or coarse-grained. A fine-grained policy can be, for example, a rule that creates a very narrowly defined filter to control the data flow on a specific network interface. A course-grained policy can, for 35 example, be a rule that creates a more broadly defined filter

DRAFT
02/20/2008
04/08/2008
05/08/2008
06/08/2008
07/08/2008
08/08/2008
09/08/2008
10/08/2008
11/08/2008
12/08/2008
13/08/2008
14/08/2008
15/08/2008
16/08/2008
17/08/2008
18/08/2008
19/08/2008
20/08/2008
21/08/2008
22/08/2008
23/08/2008
24/08/2008
25/08/2008
26/08/2008
27/08/2008
28/08/2008
29/08/2008
30/08/2008
31/08/2008
32/08/2008
33/08/2008
34/08/2008
35/08/2008
36/08/2008
37/08/2008
38/08/2008
39/08/2008
40/08/2008
41/08/2008
42/08/2008
43/08/2008
44/08/2008
45/08/2008
46/08/2008
47/08/2008
48/08/2008
49/08/2008
50/08/2008
51/08/2008
52/08/2008
53/08/2008
54/08/2008
55/08/2008
56/08/2008
57/08/2008
58/08/2008
59/08/2008
60/08/2008
61/08/2008
62/08/2008
63/08/2008
64/08/2008
65/08/2008
66/08/2008
67/08/2008
68/08/2008
69/08/2008
70/08/2008
71/08/2008
72/08/2008
73/08/2008
74/08/2008
75/08/2008
76/08/2008
77/08/2008
78/08/2008
79/08/2008
80/08/2008
81/08/2008
82/08/2008
83/08/2008
84/08/2008
85/08/2008
86/08/2008
87/08/2008
88/08/2008
89/08/2008
90/08/2008
91/08/2008
92/08/2008
93/08/2008
94/08/2008
95/08/2008
96/08/2008
97/08/2008
98/08/2008
99/08/2008
100/08/2008
101/08/2008
102/08/2008
103/08/2008
104/08/2008
105/08/2008
106/08/2008
107/08/2008
108/08/2008
109/08/2008
110/08/2008
111/08/2008
112/08/2008
113/08/2008
114/08/2008
115/08/2008
116/08/2008
117/08/2008
118/08/2008
119/08/2008
120/08/2008
121/08/2008
122/08/2008
123/08/2008
124/08/2008
125/08/2008
126/08/2008
127/08/2008
128/08/2008
129/08/2008
130/08/2008
131/08/2008
132/08/2008
133/08/2008
134/08/2008
135/08/2008
136/08/2008
137/08/2008
138/08/2008
139/08/2008
140/08/2008
141/08/2008
142/08/2008
143/08/2008
144/08/2008
145/08/2008
146/08/2008
147/08/2008
148/08/2008
149/08/2008
150/08/2008
151/08/2008
152/08/2008
153/08/2008
154/08/2008
155/08/2008
156/08/2008
157/08/2008
158/08/2008
159/08/2008
160/08/2008
161/08/2008
162/08/2008
163/08/2008
164/08/2008
165/08/2008
166/08/2008
167/08/2008
168/08/2008
169/08/2008
170/08/2008
171/08/2008
172/08/2008
173/08/2008
174/08/2008
175/08/2008
176/08/2008
177/08/2008
178/08/2008
179/08/2008
180/08/2008
181/08/2008
182/08/2008
183/08/2008
184/08/2008
185/08/2008
186/08/2008
187/08/2008
188/08/2008
189/08/2008
190/08/2008
191/08/2008
192/08/2008
193/08/2008
194/08/2008
195/08/2008
196/08/2008
197/08/2008
198/08/2008
199/08/2008
200/08/2008
201/08/2008
202/08/2008
203/08/2008
204/08/2008
205/08/2008
206/08/2008
207/08/2008
208/08/2008
209/08/2008
210/08/2008
211/08/2008
212/08/2008
213/08/2008
214/08/2008
215/08/2008
216/08/2008
217/08/2008
218/08/2008
219/08/2008
220/08/2008
221/08/2008
222/08/2008
223/08/2008
224/08/2008
225/08/2008
226/08/2008
227/08/2008
228/08/2008
229/08/2008
230/08/2008
231/08/2008
232/08/2008
233/08/2008
234/08/2008
235/08/2008
236/08/2008
237/08/2008
238/08/2008
239/08/2008
240/08/2008
241/08/2008
242/08/2008
243/08/2008
244/08/2008
245/08/2008
246/08/2008
247/08/2008
248/08/2008
249/08/2008
250/08/2008
251/08/2008
252/08/2008
253/08/2008
254/08/2008
255/08/2008
256/08/2008
257/08/2008
258/08/2008
259/08/2008
260/08/2008
261/08/2008
262/08/2008
263/08/2008
264/08/2008
265/08/2008
266/08/2008
267/08/2008
268/08/2008
269/08/2008
270/08/2008
271/08/2008
272/08/2008
273/08/2008
274/08/2008
275/08/2008
276/08/2008
277/08/2008
278/08/2008
279/08/2008
280/08/2008
281/08/2008
282/08/2008
283/08/2008
284/08/2008
285/08/2008
286/08/2008
287/08/2008
288/08/2008
289/08/2008
290/08/2008
291/08/2008
292/08/2008
293/08/2008
294/08/2008
295/08/2008
296/08/2008
297/08/2008
298/08/2008
299/08/2008
300/08/2008
301/08/2008
302/08/2008
303/08/2008
304/08/2008
305/08/2008
306/08/2008
307/08/2008
308/08/2008
309/08/2008
310/08/2008
311/08/2008
312/08/2008
313/08/2008
314/08/2008
315/08/2008
316/08/2008
317/08/2008
318/08/2008
319/08/2008
320/08/2008
321/08/2008
322/08/2008
323/08/2008
324/08/2008
325/08/2008
326/08/2008
327/08/2008
328/08/2008
329/08/2008
330/08/2008
331/08/2008
332/08/2008
333/08/2008
334/08/2008
335/08/2008
336/08/2008
337/08/2008
338/08/2008
339/08/2008
340/08/2008
341/08/2008
342/08/2008
343/08/2008
344/08/2008
345/08/2008
346/08/2008
347/08/2008
348/08/2008
349/08/2008
350/08/2008
351/08/2008
352/08/2008
353/08/2008
354/08/2008
355/08/2008
356/08/2008
357/08/2008
358/08/2008
359/08/2008
360/08/2008
361/08/2008
362/08/2008
363/08/2008
364/08/2008
365/08/2008
366/08/2008
367/08/2008
368/08/2008
369/08/2008
370/08/2008
371/08/2008
372/08/2008
373/08/2008
374/08/2008
375/08/2008
376/08/2008
377/08/2008
378/08/2008
379/08/2008
380/08/2008
381/08/2008
382/08/2008
383/08/2008
384/08/2008
385/08/2008
386/08/2008
387/08/2008
388/08/2008
389/08/2008
390/08/2008
391/08/2008
392/08/2008
393/08/2008
394/08/2008
395/08/2008
396/08/2008
397/08/2008
398/08/2008
399/08/2008
400/08/2008
401/08/2008
402/08/2008
403/08/2008
404/08/2008
405/08/2008
406/08/2008
407/08/2008
408/08/2008
409/08/2008
410/08/2008
411/08/2008
412/08/2008
413/08/2008
414/08/2008
415/08/2008
416/08/2008
417/08/2008
418/08/2008
419/08/2008
420/08/2008
421/08/2008
422/08/2008
423/08/2008
424/08/2008
425/08/2008
426/08/2008
427/08/2008
428/08/2008
429/08/2008
430/08/2008
431/08/2008
432/08/2008
433/08/2008
434/08/2008
435/08/2008
436/08/2008
437/08/2008
438/08/2008
439/08/2008
440/08/2008
441/08/2008
442/08/2008
443/08/2008
444/08/2008
445/08/2008
446/08/2008
447/08/2008
448/08/2008
449/08/2008
450/08/2008
451/08/2008
452/08/2008
453/08/2008
454/08/2008
455/08/2008
456/08/2008
457/08/2008
458/08/2008
459/08/2008
460/08/2008
461/08/2008
462/08/2008
463/08/2008
464/08/2008
465/08/2008
466/08/2008
467/08/2008
468/08/2008
469/08/2008
470/08/2008
471/08/2008
472/08/2008
473/08/2008
474/08/2008
475/08/2008
476/08/2008
477/08/2008
478/08/2008
479/08/2008
480/08/2008
481/08/2008
482/08/2008
483/08/2008
484/08/2008
485/08/2008
486/08/2008
487/08/2008
488/08/2008
489/08/2008
490/08/2008
491/08/2008
492/08/2008
493/08/2008
494/08/2008
495/08/2008
496/08/2008
497/08/2008
498/08/2008
499/08/2008
500/08/2008
501/08/2008
502/08/2008
503/08/2008
504/08/2008
505/08/2008
506/08/2008
507/08/2008
508/08/2008
509/08/2008
510/08/2008
511/08/2008
512/08/2008
513/08/2008
514/08/2008
515/08/2008
516/08/2008
517/08/2008
518/08/2008
519/08/2008
520/08/2008
521/08/2008
522/08/2008
523/08/2008
524/08/2008
525/08/2008
526/08/2008
527/08/2008
528/08/2008
529/08/2008
530/08/2008
531/08/2008
532/08/2008
533/08/2008
534/08/2008
535/08/2008
536/08/2008
537/08/2008
538/08/2008
539/08/2008
540/08/2008
541/08/2008
542/08/2008
543/08/2008
544/08/2008
545/08/2008
546/08/2008
547/08/2008
548/08/2008
549/08/2008
550/08/2008
551/08/2008
552/08/2008
553/08/2008
554/08/2008
555/08/2008
556/08/2008
557/08/2008
558/08/2008
559/08/2008
560/08/2008
561/08/2008
562/08/2008
563/08/2008
564/08/2008
565/08/2008
566/08/2008
567/08/2008
568/08/2008
569/08/2008
570/08/2008
571/08/2008
572/08/2008
573/08/2008
574/08/2008
575/08/2008
576/08/2008
577/08/2008
578/08/2008
579/08/2008
580/08/2008
581/08/2008
582/08/2008
583/08/2008
584/08/2008
585/08/2008
586/08/2008
587/08/2008
588/08/2008
589/08/2008
590/08/2008
591/08/2008
592/08/2008
593/08/2008
594/08/2008
595/08/2008
596/08/2008
597/08/2008
598/08/2008
599/08/2008
600/08/2008
601/08/2008
602/08/2008
603/08/2008
604/08/2008
605/08/2008
606/08/2008
607/08/2008
608/08/2008
609/08/2008
610/08/2008
611/08/2008
612/08/2008
613/08/2008
614/08/2008
615/08/2008
616/08/2008
617/08/2008
618/08/2008
619/08/2008
620/08/2008
621/08/2008
622/08/2008
623/08/2008
624/08/2008
625/08/2008
626/08/2008
627/08/2008
628/08/2008
629/08/2008
630/08/2008
631/08/2008
632/08/2008
633/08/2008
634/08/2008
635/08/2008
636/08/2008
637/08/2008
638/08/2008
639/08/2008
640/08/2008
641/08/2008
642/08/2008
643/08/2008
644/08/2008
645/08/2008
646/08/2008
647/08/2008
648/08/2008
649/08/2008
650/08/2008
651/08/2008
652/08/2008
653/08/2008
654/08/2008
655/08/2008
656/08/2008
657/08/2008
658/08/2008
659/08/2008
660/08/2008
661/08/2008
662/08/2008
663/08/2008
664/08/2008
665/08/2008
666/08/2008
667/08/2008
668/08/2008
669/08/2008
670/08/2008
671/08/2008
672/08/2008
673/08/2008
674/08/2008
675/08/2008
676/08/2008
677/08/2008
678/08/2008
679/08/2008
680/08/2008
681/08/2008
682/08/2008
683/08/2008
684/08/2008
685/08/2008
686/08/2008
687/08/2008
688/08/2008
689/08/2008
690/08/2008
691/08/2008
692/08/2008
693/08/2008
694/08/2008
695/08/2008
696/08/2008
697/08/2008
698/08/2008
699/08/2008
700/08/2008
701/08/2008
702/08/2008
703/08/2008
704/08/2008
705/08/2008
706/08/2008
707/08/2008
708/08/2008
709/08/2008
710/08/2008
711/08/2008
712/08/2008
713/08/2008
714/08/2008
715/08/2008
716/08/2008
717/08/2008
718/08/2008
719/08/2008
720/08/2008
721/08/2008
722/08/2008
723/08/2008
724/08/2008
725/08/2008
726/08/2008
727/08/2008
728/08/2008
729/08/2008
730/08/2008
731/08/2008
732/08/2008
733/08/2008
734/08/2008
735/08/2008
736/08/2008
737/08/2008
738/08/2008
739/08/2008
740/08/2008
741/08/2008
742/08/2008
743/08/2008
744/08/2008
745/08/2008
746/08/2008
747/08/2008
748/08/2008
749/08/2008
750/08/2008
751/08/2008
752/08/2008
753/08/2008
754/08/2008
755/08/2008
756/08/2008
757/08/2008
758/08/2008
759/08/2008
760/08/2008
761/08/2008
762/08/2008
763/08/2008
764/08/2008
765/08/2008
766/08/2008
767/08/2008
768/08/2008
769/08/2008
770/08/2008
771/08/2008
772/08/2008
773/08/2008
774/08/2008
775/08/2008
776/08/2008
777/08/2008
778/08/2008
779/08/2008
780/08/2008
781/08/2008
782/08/2008
783/08/2008
784/08/2008
785/08/2008
786/08/2008
787/08/2008
788/08/2008
789/08/2008
790/08/2008
791/08/2008
792/08/2008
793/08/2008
794/08/2008
795/08/2008
796/08/2008
797/08/2008
798/08/2008
799/08/2008
800/08/2008
801/08/2008
802/08/2008
803/08/2008
804/08/2008
805/08/2008
806/08/2008
807/08/2008
808/08/2008
809/08/2008
810/08/2008
811/08/2008
812/08/2008
813/08/2008
814/08/2008
815/08/2008
816/08/2008
817/08/2008
818/08/2008
819/08/2008
820/08/2008
821/08/2008
822/08/2008
823/08/2008
824/08/2008
825/08/2008
826/08/2008
827/08/2008
828/08/2008
829/08/2008
830/08/2008
831/08/2008
832/08/2008
833/08/

to control the data flow on a larger class or type of network interface.

Fig. 3 illustrates an embodiment of a network stack 210b that can be reconfigured during a VPN session. The VPN PC 210 can have a number of applications running on it such as applications 305. A policy store 320 serves as a repository for policies from the policy engine 126 that are updated by retrieving policies from the Access server 125 each time a VPN session is initiated. An augmented policy engine 310 is an extension of the policy engine 126 on the Access server 125. The augmented policy engine 310 uses policy rules from the policy store 320 and applies the rules to both application context priorities as well as data traffic over the network. For example, a policy rule may allow a particular word processing application on the VPN PC 210 to access a document located on the device 140 on the corporate LAN 135. The word processing program also has associated with it an application context that determines its priority in accessing the device 140. Furthermore, policy rules may apply to the network data traffic. Network flow is tracked using various factors such as the type of flow (local or remote origination), network interfaces, destination network address, and source (application, user etc.). The augmented policy engine 310 uses the application context along with the network data flow factors to enforce finer-grained packet filtering based on the policy rules in the policy store 320. In this example, the word processing application may be limited not only by the policy rule, but also by its application context and the network data traffic. The finer granularity of control prevents unwanted outsiders from accessing the VPN session. The network stack 210b stores the address space of the LAN 205 to allow the stack 210b to distinguish between devices on the SOHO LAN 205 and devices on the corporate LAN 135, and undesired nodes on the Internet or other network 120. The network stack 210b is thus able to filter packets based on the source and destination.

A socket interceptor 330 serves as a session layer component in the network stack 210b that identifies all active network applications 305. The Portable Operating System Interface UNIX (POSIX) is used to create application sockets and provide a uniform application interface. In one embodiment, the socket interceptor drops packets destined to and from certain applications 305. For example, the socket interceptor drops packets from user logins that are not authorized to be part of a VPN session. In another embodiment, the socket interceptor 330 provides context information for network packets flowing from a packet guard 360 that creates packet filters as they flow into the packet guard. In one embodiment, the socket interceptor can be implemented as a WinSock layered service provider (LSP) on a Microsoft Windows platform. In this way, the socket interceptor 330 acts as an application program interface (API) between Microsoft Windows and TCP/IP protocol software.

In addition to receiving context information from the socket interceptor 330, the packet guard 360 also creates filters from the policies in the policy store 320. The packet guard 360 also can be connected to a predetermined static configuration 365 that also provides filtering criteria. ``Instance'' filtering is dictated by the augmented policy engine 310 based on rules in the policy store 320. In one embodiment, the packet guard layer 360 can be implemented as a Network Driver Interface Specification (NDIS) intermediate driver on the Microsoft Windows platform. In this way the packet guard 360 can offer protocol multiplexing so that multiple protocol stacks can co-exist on the same host.

A Transmission Control/Internet Protocol (TCP/IP) layer that provides the network communication is connected between the socket interceptor 330 and the packet guard 360. A packet translator 350 is connected between the TCP/IP interface 340 and the packet guard layer 360. The packet translator 350 translates data packets to and from the different network locations, in this case, the packets between the corporate LAN 135 and the SOHO LAN 205. In one implementation, the packet

translator can be the Internet standard Network Address Translation (NAT) that allows a company to shield internal addresses from the Internet.

5 A network interface 370 is connected to the packet guard 360. The network interface is the session layer that interfaces the network stack 210b with network software (not shown) to connect the VPN PC 210 to the SOHO LAN 205 and ultimately to the corporate LAN 135.

10 The network stack 210b thus creates an effective ``firewall'' between the VPN session and outside intrusion.

To reconfigure the network stack 210b securely and automatically during the VPN session, the network stack 210b 405 senses the VPN session. As shown in Fig. 4, a client begins a VPN session. The network stack 210b receives 410 policies from the Access server 125 and stores 415 the policies in the policy store 320. At this point, the VPN session initially is sensed and the received policies determine what access the client, the SOHO 105 or the SOHO LAN 205, is permitted. The packet guard 360 is used to enforce 420 packet filtering. The packet filtering is performed either by receiving policy rules from the augmented policy engine 310 or by reading the pre-programmed static configuration 365 that determines what packets are filtered. Next, the socket interceptor 330 is created and provides 430 user and/or application context. The socket interceptor 330 can detect and drop 440 packets, for example, from user logins that are not permitted to be part of the VPN session. Packets from any other external PCs (not shown) also are dropped. The socket interceptor 330 also can provide 445 application 30 context information back to the augmented policy engine 320 about applications 305. This context information can be used by the augmented policy engine 310 to further enforce 420 packet filtering. Furthermore, the policies are used to filter 460 packets. Therefore, the network stack 210b is 35 constantly re-configuring itself based on policy rules received from the Access Server 125 and context information provided by the socket interceptor 330 and from the packet

5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

30

35

guard, which serves as a ``packet firewall''. The process 400 constantly monitors 450 network configuration changes throughout the VPN session to detect any external intervening and unauthorized processes.

5 Various aspects of the apparatus and methods may be implemented in digital circuitry, or in computer hardware, firmware, software, or in combinations of them. Apparatus can be implemented in a computer products tangibly embodied in a machine-readable storage device for execution by a programmable processor. The foregoing techniques may be performed, for example, by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output. The methods can be implemented in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one in/out device, and at least one output device. Each computer program may be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language. The language may be compiled or interpreted language. Suitable processors include, by way of example, both general and special purpose microprocessors. Generally, a processor will receive instructions and data from read-only memory and/or random access memory. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example, semiconductor devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM disks. Any of the foregoing may be supplemented by or incorporated in, specially designed application-specific integrated circuits (ASICS).

10 20 25 30 35

Possible advantages of the foregoing techniques include dynamic creation of a packet filtering firewall (the packet guard 360), which is driven by policies or static

configurations. Another advantage is the ability to extend policies to include application and/or user context. For example, a corporate policy may temporarily ban the use of a particular browser until patches are applied. Correlating application context and network packet flows can easily enforce such a policy. Another advantage is the ability to confirm continuously that security policies are being applied on the client side.

The foregoing method also can use unified network stack information to enforce the context-based policies. The stack is an aggregation of information across the various layers of the network stack. The combination of application and/or user context to network flow enables the fine-grained control of the network resources in the home office.

Other embodiments are within the scope of the following claims.